AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
User Records maintained by Snap Inc.

Case No. M-19-114-STE

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
Snap Inc. user records maintained by the Custodian of Records, 63 Market Street, Venice, CA 90291;

located in the Western District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:
records pertaining to Snapchat Usernames: MYSTIC MARC, TONYNELLY01; including conversations, identifying information (names, email addresses, phone numbers, etc.), any available sent or unsent photos/videos and messages;

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 875	Interstate communications

The application is based on these facts:

See Continuation Sheet.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Christopher D. Deeb, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: **Mar 7, 2019**

Judge's signature

City and state: OKC, OK

Shon T. Erwin, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Christopher D. Deeb, a Special Agent (SA) with the United States Army Criminal Investigation Division (CID), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the U.S. Army CID since August of 2014, and am currently assigned as a Special Agent to the Fort Sill CID Office. While employed by the U.S. Army, I have investigated federal criminal violations related to high technology or cybercrime, child pornography, rape, abusive sexual contact, and conspiracy. I have gained experience through training at the U.S. Army Military Police School (USAMPS) and everyday work relating to conducting these types of investigations. I have received specific training in the area of rape while I attended the Special Victims Capabilities Course (SVCC), Domestic Violence Investigation Training (DVIT), Child Abuse Prevention Investigative Techniques (CAPIT), and Advanced Crime Scenes Investigative Training (ACSIT) course with the U.S. Army, which focused on in depth investigative techniques and procedures. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b), and I am authorized by the Attorney General to request a search warrant.

2. This affidavit is submitted in support of an application for a search warrant for the contents of and information pertaining to SNAPCHAT USERNAME: MYSTIC MARC and SNAPCHAT PROFILENAME: TONYNELLY01 ("SUBJECT ACCOUNT"), which is more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities

of violations of 18 U.S.C. §§ 875 (Interstate communications); which items are more specifically described in Attachment B.

3. The statements in this affidavit are based on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 8 U.S.C. §§ 875 (Interstate communications) are located in the SUBJECT ACCOUNT.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 875(c) is defined by the Department of Justice as "Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachments A and B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

c. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

d. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

e. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

f. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

g. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

h. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

i. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

j. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

k. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

l. "Snap," as used herein, refers to a photo or video taken via the Snapchat app using the camera of a smartphone and shared with one or more individuals via Snapchat. A Snap can be accompanied with text.

m. "Memories," as used herein, refers to Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, and photos and videos from their phone's photo gallery in Memories. A user can also edit and send Snaps and create Stories from these Memories. Snaps and other photos and videos saved in Memories are backed up by Snap Inc. and may remain in Memories until deleted by the user.

n. "Selfie," as used herein, refers to a photograph that one has taken of oneself, typically one taken with a smartphone or webcam and shared via social media.

o. "Emoji," as used herein, refers to a small digital image or icon used to express an idea, emotion, etc., in electronic communication.

BACKGROUND ON COMPUTER CRIMES, THE INTERNET, AND EMAIL

6. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interact with each other. Computers basically serve four functions in connection with peer to peer interaction: production, communication, distribution, and storage.

b. With the advent of digital cameras and smartphones with cameras, when a photograph or screenshot is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer, or by wirelessly sending the digital file to another smartphone. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution

and receipt of information. Because of the proliferation of commercial services that provide chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic, or other, materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for personal information. The size of the electronic storage media (commonly referred to as the hard drive) used in smartphones has grown tremendously within the last several years. These drives can store hundreds of images at very high resolution. In addition, there are numerous options available for the storage of digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving a screenshot as a file on the computer or

saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a smartphone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

8. Individuals who use private messaging apps can use the apps to share many types of digital media, including images and videos. Many of these applications have built in features which allow the apps to access the built-in cameras on computers or smartphones to immediately capture the digital media and share it with the desired individual. This digital media is typically transferred via a Wireless Local Area Network (e.g., Wi-Fi) or a Cellular Network. Often, a record of the transmission is not recorded via SMS (or similar method) on the smartphone itself, as the app completes the transmission without utilizing SMS.

9. In my experience, I know individuals use these capabilities to send images and videos which depict sexually explicit material and contain evidence of criminal offenses.

10. I also know that individuals often find ways to capture images or messages for exploitation, either by saving the digital media onto their computers and/or smartphones, or taking still photographs (including "screen captures" or "screen shots") of the digital media.

TECHNICAL INFORMATION REGARDING SNAPCHAT

Snapchat

11. Based on my training and experience, and publicly available information, I have learned that Snap Inc. provides a variety of on-line services, including private messaging services, to the general public. Snap Inc. allows subscribers to engage in "chats" with other Snapchat users. A user can type messages, send photos, videos, audio notes, and video notes to friends within the Snapchat app using the Chat feature. A user sends a Chat message to a friend, and once it is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message that they want to keep. The user can clear the message by tapping it again.

12. Snapchat also allows a user to take "Snaps." A Snap is when a user takes a photo or video using their camera phone in real-time and then selects which of their friends to send the message to. Unless the sender or recipient opts to save the photo or video, the message will be deleted from their devices (after the content is sent in the case of the sender and after it's opened in the case of the recipient). Users are able to save a photo or video they've taken locally to their device or to "Memories," which is Snapchat's cloud-storage service.

13. Memories is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. A user can also edit and send Snaps and create Stories from these Memories. Snaps, Stories, and

other photos and videos saved in Memories are backed up by Snap Inc. and may remain in Memories until deleted by the user.

14. In my training and experience, generally, providers like Snap Inc. ask each of their subscribers to provide certain personal identifying information when registering for a Snapchat account. Per Snap Inc., this information can include the subscriber's Snapchat username, email address, phone number, Snapchat user vanity name, Snapchat account creation date and IP address, and Timestamp and IP address of account logins and logouts. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

15. The mobile number and email address provided to Snap Inc., by the user is particularly useful a user needs to recover his/her account in the event of a lost password or account compromise. Because a mobile device number and email address is linked to an account, it tends to be closely associated with the user of the account. It is important to note that the input requires voluntary input from users. As this additional input is voluntary, Snap Inc. is not always successful in validating a user's personal identifying information.

16. When creating an account at Snapchat, the user is provided the opportunity to create a vanity name and an associated "Profile." Snap Inc. allows a user to personalize their Profile by "adding an image that represents you." The vanity name and display image a user

provides for their Profile is public and can be seen by anyone, even if the user chooses to keep the rest of their Profile hidden from other users.

17. In the Snapchat Law Enforcement Guide, Snap Inc. states they typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the IP address used to create the account, a timestamp and IP address of account logins and logouts, and a list of current historical Snapchat user vanity names.

18. In my training and experience, Snapchat users often use Snapchat accounts for everyday communications because it is fast, low cost, private, and simple to use. People use messaging services to communicate with friends and family, and to stay informed of their family and friends' activities. Snapchat users are able to store records of these communications in their Snapchat accounts, which may include personal identifying information such as name and address.

19. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with a Snapchat account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, electronic messaging communications, and images sent (and the data associated with the foregoing, such as date and

time) may indicate who used or controlled the account at a relevant time. Further, information maintained by Snap Inc. can show when and where the account was accessed or used. For example, as stated in the Snapchat Law Enforcement Guide, Snap Inc. typically logs the Internet Protocol (IP) addresses from which users log into their Snapchat account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the Snapchat account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored in the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent Snapchat). Lastly, stored electronic data may provide relevant insight into the Snapchat account owner's state of mind as it relates to the offense under investigation. For example, information in the Snapchat account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

PROBABLE CAUSE

20. On 7 Feb 2019, Ms. T.S. provided a statement to this office, wherein she described how she, and her daughter, were threatened via the cell phone application, Snapchat. Ms. Smith provided details how she was contacted by an unknown individual, who "Friend Requested" her. Ms. T.S. stated she accepted the friend request and immediately started receiving threatening messages. Ms. T.S. began "screenshotting" the messages, as well as the

sender's "Profile Page". Ms. T.S. provided these images to CID, who initiated the investigation. It should be noted that Ms. T.S. was the victim in a previous rape and sexual assault investigation, wherein she was assaulted by four Soldiers stationed at Fort Sill, OK. The incident was investigated by the Fort Sill CID office.

21. Ms. T.S. provided the screenshots she kept on her cell phone of the messages. The profile name of the sender of the message can be seen, which read "Mystic Marc". Ms. T.S. accessed the profile page for the individual which revealed the username: "tonynelly01".

22. Two messages sent to Ms. T.S., which were captured in the screenshots and provided to this office related the following messages: "Something will happen to your daughter", and "now there's nothing to lie about .. I'm sure you stay in that same house too..".

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

23. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 875 (Interstate communications), by using the warrant to require Snap Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

JURISDICTION

24. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) &

(c)(1)(A). Specifically, this Court is a "district court of the United States (including a magistrate judge of such court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

25. I request that the Court order that all papers submitted in support of this application, including this affidavit, the application, the warrant, and the Order itself, be sealed until further order of the Court, except that a copy of the warrant, including its attachments, shall be served upon Snap Inc. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, or otherwise seriously jeopardize the investigation.

CONCLUSION

26. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on computer systems owned, maintained, controlled and/or operated by Snap Inc., there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the electronic account described in Attachment A. The facts outlined above show that the SUBJECT ACCOUNT listed in Attachment A has been used to communicate with person(s) for the purpose of communicating threats to Ms. Smith and others. There is probable cause to

believe that the subjects of this investigation did violate the aforementioned statutes under Federal law.

27. Because the warrant will be served on Snap Inc., who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Christopher Deeb
Special Agent
U.S. Army Criminal Investigation Division

Subscribed to and sworn before me this 7TH day of MARCH, 2019.

Shon T. Erwin

HONORABLE SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

This warrant applies to the contents of and information associated with SNAPCHAT USERNAME: TONYNELLY01, SNAPCHAT PROFILE NAME: MYSTIC MARC, Snapchat accounts that are stored at premises controlled by Snap Inc., a company that accepts service of legal process at 63 Market Street, Venice, California 90291.

ATTACHMENT B

Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by Snapchat (the "Provider") to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of Snap Inc., including any records, files, logs, or information that have been deleted but are still available to Snap Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on 21 February 2019, Snap Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A, including any information contained in that account which is helpful to determine the account user's or owner's true identity:

a. All records or other information regarding the identification of the accounts, to include full name, email address, telephone numbers, current and historical vanity names, records of account creation, the IP address used to register the account, and log-in IP addresses associated with session times and dates from January 2019 through March 2019;

b. The contents and logs of "Snaps" between SNAPCHAT USERNAME: MYSTIC MARC and/or TONYNELLY01 and any Ms. T.S. who provided her SNAPCHAT SUERNAME: SMILEYBATMAN, between the dates for the first week of February 2019 (1 February 2019 through 7 February 2019); to include all available sent and received logs, any unopened chats, any chats saved by the sender or recipient, the content of any chats saved by a sender or recipient, and any metadata available;

c. The contents of all "Memories," to include sent or unsent Snaps, photos, and videos.

The Provider shall deliver the information set forth above via United States mail, courier, or e-mail to:

SA Christopher Deeb
Fort Sill CID Office
2635 Miner Road
Fort Sill, OK 73503
Christopher.d.deeb.mil@mail.mil

II. Information to be seized by the government

1. All information described above in Section I that constitutes contraband or fruits, evidence or instrumentalities of violations of Title 18 U.S.C. §§ 875 (Interstate communications); including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Whoever transmits in interstate or foreign commerce any communication containing threat to kidnap any person or any threat to injure the person of another;

b. Evidence indicating how and when the Snapchat account was accessed or used, to determine the geographic and chronological context of account access, use, or events relating to the crime under investigation and to the account owner or user;

c. Evidence indicating the Snapchat account user's or owner's state of mind as it relates to the crime under investigation.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Snap Inc., and my official title is _____. I am a custodian of records for Snap Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Snap Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Snap Inc.; and

c. such records were made by Snap Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature